OFFICE OF THE MANAGER
NATIONAL COMMUNICATIONS SYSTEM

INFORMATION SECURITY BUSINESS CASE

CASE STUDY #4 - AMBASSADOR

5 June 1997

Further distribution only as directed by
Office of the Manager,
National Communications System (OMNCS)
Customer Service and Information Assurance Division
Information Assurance Branch (N53)

DCA100-95-D-0104
Delivery Order No. 10
Information Security Business Case
Case Study #4-AMBASSADOR

ABSTRACT

This case study was prepared as part of a larger effort to develop a business case approach to justify funding for network security programs. The Government sponsor of the project selected the case study participant from a list of candidates developed by the SAIC project team. The case study presents an overview of the participant organization, including its technical and operational environments; discusses the motivation for establishing a security program; describes the organization's Network and Information Security Program; overviews the participant's business case process; and presents senior management's view of several network and information security issues.

TABLE OF CONTENTS

LIST OF TABLES

DCA100-95-D-0104
Delivery Order No. 10
Information Security Business Case
Case Study #4-AMBASSADOR

1. INTRODUCTION

In recent years, information and telecommunications technology and services have expanded at an astonishing rate, in terms of the technology and implementation. The public and private sectors increasingly depend on information and telecommunications systems capabilities and services. In the face of rapid technological, regulatory, and societal change, public and private organizations are also undergoing significant changes in the way they conduct their business activities, including the use of wide area networking via public networks. These changes include mandates to reduce expenses, increase revenue, and return on investment, in order to compete in a global marketplace. Even under prosperous economic times, security has not been easy to sell to upper management unless the organization has been the victim of a major security incident or the marketplace demands it. In today's business environment it is even more difficult to obtain senior management approval to justify the expenditure of valuable resources — yet, this expenditure is necessary to guarantee that a potentially disastrous event will not occur and affect the ultimate survivability of an organization.

SAIC has been tasked by the Office of the Manager, National Communications System (OMNCS), Customer Service and Information Assurance Division, Information Assurance Branch (N53) under the Defense Information Systems Agency (DISA) contract DCA100-95-D-0104, Delivery Order 10, to provide the Government with a report and briefing supporting the justification of funding network security related programs. The purpose of Task 2 of this delivery order is to research, develop, produce, write, and publish three individual case studies of organizations that have been the victims of significant intrusions and have initiated significant programs afterward to improve security within their networks. A fourth study was added as a target of opportunity when an organization revealed interest in participating in the cast study process. This report represents that fourth study.

To protect the anonymity of the organizations in the case studies, a code name has been assigned to each organization. The code name of the fourth case study organization is AMBASSADOR.

1.1 Purpose of the Project

The overall purpose of the Information Security Business Case project is to research, develop, produce, write, and publish a Business Case for Security. The project consists of performing research on organizations that have been the victims of significant network intrusions or related network assurance incidents or have initiated significant programs to improve security within their networks and systems for other reasons such as deregulation of an industry sector or direction of a corporate board of directors. The final product will be a “generic” approach/methodology for justifying network and information systems security expenditures.

1.2 Approach for Performing the AMBASSADOR Case Study

The first step in performing the AMBASSADOR case study was obtaining the consent of the organization’s senior management to be a participant. The case study point of contact was the Director Business Assurance. Once an oral agreement was obtained, SAIC and the participant executed a non-disclosure agreement to ensure the organization’s anonymity. SAIC developed a questionnaire guide to be used during the initial data collection effort. A team of three SAIC personnel conducted a 2-day on-site visit to the participant organization and interviewed the point of contact, his supervising Vice President, and the Director’s staff members using the questionnaire guide. During the interview, the SAIC team identified several pertinent documents and requested copies. Documents collected during the interview included policies, procedures, code of conduct statements, network schematics, business case studies, and awareness materials. The SAIC principal investigator held several follow-up telephone conversations with the AMBASSADOR point of contact to answer questions and to obtain additional data relevant to the case study. The SAIC team gathered background material concerning the participant organization both from the participant and from open sources.

1.3 Overview of the Report

Section 2 describes the business services and the technical and operational environments of AMBASSADOR. Section 3 depicts the activities that motivated AMBASSADOR to develop a network and information security program. Section 4 provides a description of the evolving network and information security program, including the security organization and the security policies. Section 5 describes the informal business case process used by AMBASSADOR. Section 6 provides the lessons learned by management in navigating the AMBASSADOR enterprise network infrastructure through the dangers of a telecommunications network intrusion, outage, or denial of service.

2. OVERVIEW OF THE AMBASSADOR ORGANIZATION

2.1 Description of the Business

Originally a local telephone company, AMBASSADOR is now a worldwide company with a diverse range of information processing systems.. AMBASSADOR’s local, long-distance, Internet service provider, and wireless subsidiaries provide integrated communications services to 10 million customers nationwide. The company’s combined wireless, wireline local and long-distance revenues rank it in the top five telecommunication companies in the United States today. AMBASSADOR is at the forefront of the new communications, entertainment and information industry. Globally, it is one of the largest investors in the high-growth wireless communication marketplace and is actively developing high-growth national and international business opportunities in all phases of the industry. The company’s Large Business Services organization offers customers integrated voice, data, and video applications and professional consulting and support services that add up to a precise solution □ a solution that fits and evolves to meet customers’ specific communications needs.

AMBASSADOR is a visionary proponent of Telecom Age security and privacy. Its 3-year-old privacy code includes six guiding principles:

- It will only collect information about customers in an effort to serve them better.
- It handles personal information based on the sensitivity of the information and established disclosure practices.
- It will give customers access to information it has about them, and will explain its business practices concerning this information.
- It will ensure its employees’ compliance with these guiding principles. Employees will be accountable for the proper use of customer information and AMBASSADOR will assess privacy impacts in developing new products and services.
- AMBASSADOR will participate in the public policy debate on information privacy issues, and will support the development of international standards to protect personal information and its proper use on a worldwide basis.

- AMBASSADOR's Privacy Code will not be stagnant, but dynamic, and will continue to evolve as new products, services and challenges emerge.

As a blueprint for action, AMBASSADOR senior management believes that, "All participants □ those who build the information roadways, those who provide services, users of services, and government entities □ should work cooperatively to ensure privacy and security issues are addressed now."

As stated earlier, AMBASSADOR serves several million customers in its current base and plans to expand that customer base within its serving areas, as well as into national and international markets. The company provides local, long-distance, and global calling services, wireless communications, video-on-demand, network and information management services, Internet services, and teleconferencing. AMBASSADOR's Wireless business unit was recently singled out for its extensive coverage area and its wide variety of service plans. The company offers a full range of wireless personal communications services, including voice, data, and paging. It recently launched the wireless industry's most sophisticated digital cellular phone service in its operating area. The new offering uses 13-kilobit Code Division Multiple Access (CDMA) to provide exceptional voice quality and enhanced security. This AMBASSADOR business unit also provides secure wireless data transmission via encrypted Cellular Digital Packet Data (CDPD) in major cities across the region it serves.

With the announcement of AMBASSADOR's long-distance operations, mergers, and acquisitions it is also deploying a Full Service Network (FSN). This state-of-the-art "fiber-to-the-curb," switched broadband network consists of fiber optics and new electronic technology □ providing customers with reliable and higher-quality telephone service. The network also supports future services, such as high-speed home access to the Internet and computer networks, digital broadcast and interactive TV, video-on-demand, medical imaging, and distance learning.

AMBASSADOR is organized into nine business units. Table 1 provides the units and their primary services.

Table 1. Business Units

BUSINESS UNIT	SERVICES
Wireless Unit	Provides wireless services such as cellular phone and paging.
Internet Services	Provides a full range of information, communications and publishing services.
Long-Distance Services	Provides local, competitive local, interstate, and international calling services.
Network Services	Builds, installs, repairs and manages telecommunications networks and advanced services, e.g., ADSL, ATM, SMDS, ISDN, SONET, Digital Line Carrier and Full Service Networking for AMBASSADOR consumer and business customers.
Video Services	Provides Video-On-Demand (VOD) service allowing customers to retrieve, on demand, videos stored on computer servers, much as they retrieve electronic mail messages.
Local Exchange Carrier	Serves residential and business customers inside of its operating territories.
Federal Systems	Provides advanced intelligent voice, data networking, infrastructure and systems integration solutions with established contractual platforms, multi-disciplinary federal market specialists, and a reputation for secure, reliable, quality service.
Public and Operator Services	Provides Operator Services for AMBASSADOR wireline and wireless customers. Wholesale Operator Services for major satellite, wireless and wireline carriers across the United States.

2.2 Description of Network and Information Systems Environment

The information and network technology used to support AMBASSADOR’s Corporate backbone network environment and all of the core businesses units is a distributed, heterogeneous environment. A plethora of legacy systems support its core telecommunications operations. The AMBASSADOR Corporate distributed backbone network supports various applications and enterprises, including the business units identified in Table 1. The backbone network is made of two main sub-networks, one supporting the regulated Public Switched Network (PSN) telephone company while the other supports the various unregulated enterprises. These networks are tied together by local and wide area networks and secure trusted gateway domains. Connectivity to the Internet is through one or more of the Checkpoint Firewall 1 VPN Authenticating firewalls running on Sun Ultra1 platforms. The PSN Operations Systems network and the trusted gateway domain platform consists of Cisco 7505 routers with FDDI, and Fast Ethernet networking.

3. MOTIVATION(S) FOR ESTABLISHING SECURITY PROGRAM

Two compelling events related to PSN operations caused the security program within AMBASSADOR to develop significantly in both scope and depth. The first incident/event occurred during a post-mortem of a major outage of the PSN in the early 1990s. Although it was later determined that the outage was not caused by a security incident, the investigation team found software security and change control to be seriously deficient within the affected signaling network elements. Deficiencies in separation of responsibilities, least privilege, and audit logging were also cited and addressed during the investigation. As a direct byproduct of the major PSN outage investigation, AMBASSADOR established a multi-disciplined operations review effort to audit and test its security programs. That review effort, led by Bellcore, involved key personnel from all areas of AMBASSADOR's PSN operations and its Internal Audit organization.

A second, more recent, compelling event supporting the security program within AMBASSADOR involved contingency planning for a work stoppage. Potentially serious inadequacies in the effectiveness of planning for such an event were detected and reported to management, as part of AMBASSADOR's extensive internal audit program. The audit found that virtually all of the trained technicians responsible for day-to-day operations of the PSN nodes were non-management employees represented by a collective bargaining unit. Should a work stoppage have occurred, there would have been no way to control access while ensuring PSN continued operations support. The risk analysis conducted as part of that contingency planning audit determined that Network Elements of AMBASSADOR's PSN were at considerable risk from disgruntled technicians. The analysis also found that AMBASSADOR was dependent upon remote PSN operations, administration, maintenance and provisioning (OAM&P) systems networking and personnel upon which could be exploited if additional physical and logical access controls and countermeasures were not put into place.

Customer confidence and trust in the integrity, security, and reliability of AMBASSADOR's PSN service offerings and internal systems supporting the PSN are the **number one** business driver for AMBASSADOR's security program. This level of commitment to security, coupled with increased customer and regulatory interests in security of the PSN, have caused AMBASSADOR's audit and compliance programs to take an expanded look at computer and network security regularly.

Although not specifically required within the current legal environment, the AMBASSADOR computer security program is recognized and highlighted within the AMBASSADOR Federal Sentencing Guidelines Compliance Program. AMBASSADOR's Legal Department maintains an active Compliance and Code of Business Integrity Program. This program includes hotline reporting and a referral program along with a quarterly integrity newsletter issued to all employees. The Integrity Newsletter offers employees a periodic, informational, and quiz-based vehicle to keep abreast of current Code of Conduct issues, concerns, violations, and hypothetical situations. Of the last six issues, three contained extensive coverage of computer and network security issues, incidents, policies, and programs. Other subjects covered in the newsletter ranged from Equal Employment Opportunity to Foreign and Corrupt Practices Act Compliance. Each issue of the newsletter contains the listing of important contact numbers to report an incident, and to seek information or counsel. By including Computer Security issues periodically within the Code of Business Integrity program and integrating its results with the Federal Sentencing Guidelines Compliance Program, AMBASSADOR is sending an important message to its employees to act within the highest ethical and legal standards. AMBASSADOR is forward-looking in its support of the U.S. Federal Sentencing Commission's Guidelines, which recently added language to address violations of the federal computer crime statutes and recent amendments to the statutes.

As a direct byproduct of the major PSN outage investigation, the AMBASSADOR Internal Audit organization significantly increased its annual assessment coverage of PSN computer and network security and business assurance operations. In addition, the Information Security Enforcement (ISE) function has been added to the AMBASSADOR Business Assurance organizational responsibilities. The Integrity Newsletter publishes results of the ISE Project Safeguard vulnerability and readiness assessments against AMBASSADOR policies and guidelines periodically. As an example, the First Quarter 1996 newsletter described the results of an ISE baseline test of 20,000 UNIX□ workstations and administrators. In addition, the article described administration responsibilities, available security tools, mailing lists and incident reporting hotline numbers. (**NOTE**: At least three different numbers are listed in the Integrity newsletter, which may dilute the message and effectiveness of the AMBASSADOR Compliance Program.)

One of the secondary motivations for sustaining AMBASSADOR's network and information security program is to allow AMBASSADOR Business Assurance and Engineering operations the ability to detect, contain, and deter incidents or intrusion into its internal business platforms supporting the PSN. To support that capability, several major programs are under way to enhance access control, offer single sign-on solutions, and prepare the company for increased diversification of its service offerings across a full service network digital ATM based infrastructure.

In the last 18 months, several significant incidents were recognized, reported, and investigated.

The first case involved intrusions into a PSN electronic switching system switch known as 1AESS from AT&T. The incident was first detected when AMBASSADOR Corporate Security received a call from the security organization of a major exchange carrier requesting information on suspected fraudulent calls to what appeared to be an AMBASSADOR testline number. The number was assigned to the dial-back-up link (believed to have been taken out of service several years ago). This link is attached to the maintenance port of the UNIX-based attached processor of one of AMBASSADOR's 1AESS end office switching systems. Further investigation by the major exchange carrier revealed that not only was the suspect intruding into the AMBASSADOR switch, but also the intrusion and subsequent unauthorized call forwarding entries into the switch database were being broadcast through a video teleconference arrangement to other hackers. The incident has been referred to law enforcement and is pending prosecution. A second, more experienced intruder into the 1AESS was also detected during the investigation, editing the Recent Change database to affect call forwarding changes and provision of a 1FR residence line. To minimize the risk of further intrusion, the dial-back-up facility was taken out of service and periodically monitored. Law enforcement has been notified and a criminal investigation is underway. As a result of the incident, AMBASSADOR also launched an audit review of all 1AESS offices. Total cost of the investigation to date is estimated to be six staff weeks. In addition, under an existing contract with Bellcore for forensic assessment and containment consultation, AMBASSADOR authored a bulletin to other PSN service provider clients of the Network Security Information Exchange.

A second case involved ongoing intrusion attempts into AMBASSADOR diagnostic test units known as Direct Access Test Units (DATU) from Harris Corporation's Dracon Division. The unit has the ability to perform intrusive tests of customer lines. While the line is being tested it is taken out of service, causing a temporary loss of service to the associated subscriber. The DATU uses a tone insertion scrambler to mask out intelligence, so it is not believed to be useful to intruders in monitoring a customer's line. A total of two staff weeks has been spent to date on these DATU incidents and allegations, but it is expected to be a recurring area of concern.

A third case involved indications of social engineering to affect PSN network access and service changes. The case was brought to light in connection with the arrest and conviction of a member of the Internet Liberation Front (ILF), a hacker group believed responsible for intrusions into telephone company operations in the Mid-West. Analysis of the hacker's notebook revealed that it contained detailed information such as names, telephone numbers, and business function of local and long-distance telephone companies, centers, personnel, modems, and operations across the nation. The hacker used an asterisk next to a name to convey that an employee was "very friendly" and thus vulnerable to social engineering. It is unknown at this time what risk factor should be associated with this case except to use it as an instrument in employee awareness of the social engineering intrusion threat.

Another case involved an employee who unknowingly posted proprietary information on network configuration and addresses to the Internet news group looking for help on a problem. The employee was advised of the serious nature of such an oversight and warned to be more cautious in the future.

Another case involved an incident of an employee in Operator Services who was believed to be downloading the Operator Services position system screens and databases onto his personal laptop. He was observed by one of his co-workers looking at listings on his laptop system. An interview of the suspect and voluntary search of his home PC found nothing. The employee was subsequently terminated for poor performance not related to the investigation.

4. AMBASSADOR’s NETWORK AND INFORMATION SECURITY PROGRAM

4.1 Organizational Location and Reporting Chain

The Executive Director, Disaster, Recovery and Security reports directly to the Chief Information Officer (CIO). The organization is centrally located within Ambassador with sufficient interfaces to the business units and other internal organizations.

4.2 Network and Information Security Staff

The total network and information security staffing is 38 with expected additions planned as a result of business function expansion to incorporate disaster recovery and planning.

4.3 External Interfaces

Ambassador interfaces with several external security organizations/associations to include membership in TSARS.

4.4 Corporate Information Security Policies and Procedures

AMBASSADOR has a comprehensive set of Corporate Information Security policies and guidelines. These policies and guidelines have been approved by Ambassador’s Chairman of the Board and distributed widely in written and electronic form on AMBASSADOR’s internal website. They govern virtually every step in the life cycle of safeguarding computer-based information systems and resources, including the acceptable use of and protection of all AMBASSADOR information, computing, and networking resources. The guidelines are based upon the AMBASSADOR Employee Code of Business Conduct. The set of guidelines and reiterated policies state the fundamental information security rules, expectations, rewards, penalties for non-compliance, and responsibility to acknowledge and comply with the stated principles and policies. The policies address 13 specific areas:

- Objective and Scope of the Policy
- Responsibilities and Expectations on Compliance: General, information security organization, management, individual/user, administrators, software engineers, third parties, etc.
- Personal Computers and Intelligent Workstations
- Communications Networks: General network management, dial-up access, firewalls, internetworking
- Software: Uses, licenses, and safeguards
- Information Assets: Classification of data, proprietary nature and customer proprietary network information notations, ownership responsibilities, access controls, and security classification
- Product and Application Development: Risk assessments, lifecycle controls, development and deployment, customer access, integrity controls, and compliance reviews
- Audit Trails and Reports: Logs, archive, and retention
- Physical Security
- Contingency Planning and Disaster Recovery
- Security Incident Handling
- Company Markings: Copyrights, proprietary markings, and warning banners
- Glossary of Terms
- Appendix B, Selected Internal Security Practices.

4.4.1 Fundamental Corporate Information Security Policy. The fundamental policy statement states that: *"It is the policy of the company to provide protection for all corporate computer and computer network assets commensurate with their value to the company, their potential for misuse, and current industry practice. The Company will plan, design and maintain systems and networks so as to ensure privacy, accuracy, integrity and continuous availability."*

4.4.2 Information Classification. This policy identifies and defines two data classifications that are to be used to categorize all proprietary data. The categories are: **NOTICE and, Private** Restricted Distribution, Use and Availability.

Table 2. Information Classification

CLASSIFICATION	DEFINITION
NOTICE	Proprietary: Not for Use or Disclosure Outside of the AMBASSADOR Enterprise Except Under Written Agreement
Private	Sensitive Proprietary Information The Information Contained Herein Is Intended Solely for Use of those Employees of AMBASSADOR Companies who have a NEED TO KNOW the subject matter. Disclosure to others is PROHIBITED. DO NOT REPRODUCE

4.5 Information Security Program Costs

The cost of the information security program is approximately $13 million, with $10 million allocated for expenses and $3 million for capital.

4.5.1 Costs Associated with Initial Incident. The costs associated with the initial major incident, a non-security related outage of the Public Switched Network, included $100k in investigation costs with several million dollars spent on additional research and $250k in additional systems security and interoperability testing. Other incidents such as the switch intrusion case resulted in $18k in labor charges for the investigation and a $10k audit of 1AESS ports. The social engineer case has resulted in $10k in labor and travel expenses to date.

5. AMBASSADOR BUSINESS CASE PROCEDURES

AMBASSADOR is a commercial enterprise competing in a rapidly changing regulatory, technological, and marketplace environment. In order to survive and compete effectively, AMBASSADOR must base its potential investments on sound business, financial, and economic analyses. In today's information services environment, there is increasing pressure on contribution to the bottom line, cost-reductions, and revenue growth. As critical as information security and assurance may appear to be to AMBASSADOR's business operations, each expenditure over $1 million dollars requires a comprehensive business case analysis. In addressing the critical need of information assurance and disaster recovery for its data centers, an eight-page decision support document was created and accepted by AMBASSADOR's senior management for authorization of the $10 million dollar project. The organization of that business case decision support document was as follows:

- *Executive Summary* - Briefly described the need and proposed solution in terms of current situation, risk exposure to natural and malicious acts, impact and issues closure to be addressed by the suggested solution. To appreciate the cost minimization and interdependency with other major data center business cases, the executive summary referenced the specific cases and value-added benefits and interdependencies of the project.
    - *Approach* - Described the strategy and document methodology to address a Business Impact Analysis (BIA) performed earlier by one of the Big-8 Accounting Firms.
    - *Strategic Assessment* - Established the scope of the project to address the recovery and information protection of critical business applications (billing and collections, carrier interconnection, maintenance and repair, federal systems, and large business services) and PSN Operations Support Systems (SS7 databases and OSSs, Operator Services databases, E-911 databases and regional network OSSs), residing within AMBASSADOR data centers.
    - *Economic Analysis* - The BIA estimated loss of just three of the five critical business applications was determined to be $8 million per day. The BIA loss for the other seven critical functions or systems were not readily quantified but are viewed as

mission critical to supporting AMBASSADOR's regulated and non-regulated customers.

- *Program Management* - The project was based upon a six-phase implementation: Recovery contracts, project kickoff, implementation of recovery sites, application recovery and testing, recovery program build-out, and acceptance.
- *Program Schedule* - The project solution was to be implemented over a 1-year period.
- *Conclusions* - Provided both the bottom line justification and good will aspects of project approval and timely implementation.

The project was approved by AMBASSADOR senior management and recently moved into the execution phase.

6. AMBASSADOR MANAGEMENT VIEW OF SECURITY

The Chief Information Officer (CIO) of AMBASSADOR was interviewed regarding senior management's view of the security issues facing the company. According to the CIO, AMBASSADOR senior management and the Board of Directors view security as a vital issue facing the company. Interviews of the General Internal Auditor (GIA) and the CEO of AMBASSADOR's Federal Systems are scheduled but not complete as of the date of this report.

The Chief Financial Officer (CFO) is the guardian and champion for security across the AMBASSADOR enterprise and regularly reports to the Board on security policies, issues, and incidents. As a matter of fact, the CIO stated that he has been "called to the carpet" more times to security issues than any other operational issues.

A major issue facing AMBASSADOR is the opening of operations support systems to competitors as a result of open market deregulation unbundling, interconnection, and access mandated by the Telecommunications Act of 1996. Making these systems available to competitors certainly makes the local more vulnerable to exploitation, largely owing to the lack of existing technology and security domains within the operations systems networks that support the PSN. The move toward intelligent networks where system control is distributed across the network will also place the operations systems at risk. It is AMBASSADOR's view that the magnitude and security implications of unbundling of the network elements are not well understood by the industry, even given the efforts by industry forces such as the NRIC to address these implications. The implication is that security of the public networks will be placed at greater risk. This is entirely understandable since the partitioning necessary to allow secure, reliable access to UNE to a large part does not exist even in the standards bodies. The CIO is very concerned over the unbundling and increased interconnection to the SS7 network, the control network for the public switched network.

Because of the AMBASSADOR's longstanding concern about security issues, owing in part to the customers it serves, all employees are sensitive to a continuing threat to AMBASSADOR's systems and networks. AMBASSADOR has built its trusted network systems employing the latest in security techniques, technologies, firewalls and systems. Unbundling of the operations support systems will also place this trusted network at risk, since the potential threats will be coming from behind the firewalls of the trusted network systems. Although AMBASSADOR is moving toward the establishment of network domains and granting access to the domains on a need-to-know, need-to-access basis, it is by no means a trivial re-architecture engineering process. AMBASSADOR senior management considers the company reasonably well protected, in a relative sense. However, they also know that the threat is ever present and must be addressed.

AMBASSADOR treats security as a cost of doing business. Security investments are justified by using the business case model use for all capital investments.

AMBASSADOR views mergers of the large telecommunications companies a continuing fact of life. From a global perspective, they see five or six giants emerging, each with revenues of over $50 billion. These continuing mergers also have significant security implications as differing security philosophies, responsibilities, accountabilities, techniques, and technologies are merged.

The CIO concluded with AMBASSADOR's message to the industry □ the industry is vulnerable! Security must be an ongoing concern and reviewed in detail annually during which multi-disciplined quality teams review their security posture and exposure. The security posture of a company is very dynamic. When implemented, changes in business practices and technology, introduction of new applications, mergers and acquisitions, and such factors invalidate the perceived security posture. Business cases for all investments must address security implications and costs. To mitigate that vulnerability at least an annual, detailed review of the security posture is absolutely essential.